REMARKS

Claim Objections

Claim 8 has been amended in accordance with the Examiner's suggestions (Detailed Action, paragraph 3a).

Claim 9 has been revised to incorporate the features of the processor of claim 8 in the apparatus of claim 9 in a manner that clarifies the structure of the apparatus and the various memories recited therein. By this amendment, the Applicant believes that the objection raised against claim 9 (Detailed Action, remainder of paragraph 3) has been addressed.

Claim Rejections

The Examiner has maintained the rejection of claims 1-2 and 6-13 under 35 U.S.C. 103(a) as being unpatentable over Mirov et al., U.S. Patent No. 6,138,236 ("Mirov") in view of Cooper et al., U.S. Patent No. 5,805,882 ("Cooper"), and the rejection of claims 4, 5 and 14-20 as being patentable over the allegedly admitted prior art in view of Mirov and Cooper. The Applicant respectfully traverses this rejection for the following reasons, which apply to all claim rejections:

The cited art, alone or in combination, does not teach a verification step that is independent of the code content of flash memory

In response to the application of Mirov and Cooper, and in reply to the Examiner's response to the Applicant's previous arguments (Detailed Action, page 13), the Applicant submits:

Mirov describes that:

> During initialization of the computer system 10, the secure micro-code 51 of the authentication section 45 executes and directs the hash generator 53 to generate a data hash of the unsecured micro-code 58 programmed in the programmable section 55 of the flash PROM 18. The secure micro-code 51 also directs the decryptor 54 to calculate a verification hash. The decryptor applies the public key 56 of the authentication section 45 and the digital signature 57 of the programmable section 55 and calculates the verification hash.
>
> Once the verification hash and the data hash are generated, the micro-code 51 directs the comparator 52 to compare the verification hash with the data hash. (Mirov, col. 4, lines 8-20)

Cooper describes that at a first step,

> ...the microcontroller 174 checks the integrity of the flash ROM 122 by performing a checksum computation on the bottom-most 16KB segment of the flash ROM 122 content. The checksum is preferably determined at step 206 by adding, without carry, the lowest 8,192 16-bit words of the flash ROM 122... If the flash ROM 122 segment passes the checksum test, the routine proceeds to step 210. Alternatively, if the flash ROM 122 checksum indicates a failure in step 206, the flash ROM 122 has been corrupted and needs to be reprogrammed in step 208. (Cooper, col. 9, lines 30-46)

Both Mirov and Cooper both teach some type of comparison or checking step, the outcome of which is dependent on the content of the code stored in flash memory: in Mirov, the comparison requires that a hash of the flash memory's content be computed; in Cooper, a checksum is performed on the bottom-most 16KB segment.

If, as the Examiner stated, one were to conclude that it were open to a person having ordinary skill in the art to combine the teachings of Mirov and Cooper—a point which the Applicant does not concede, and respectfully traverses—then the skilled worker would arrive at a system such as that of Cooper, except that the checksum computed from a portion of the memory would be replaced by a computation of a hash from the content of the memory, which would then be compared to a decrypted value. Both references, whether separate or combined, thus teach away from the present claimed subject matter. The claims currently presented do not rely on the program code stored in the flash memory in order to derive a value for a comparison or checking step; the comparison is therefore not dependent on any extra steps, unlike Mirov or Cooper.

The Examiner equated "predetermined", as used in the pending claims, with a verification hash, in that the outcome of a hash derived from a given set of data is predictable and will always yield the same value (Detailed Action, page 13, paragraph 26). The Applicant submits that regardless of the fact that a hash may always yield the same value, neither Mirov nor Cooper, alone or in combination, teach the "predetermined security value" of the pending claims; the "predetermined security value" recited in the claims is not a value dependent on the content of the flash memory, but may be ***independent*** of the content of the flash memory. For example, paragraph 30 of the application as published describes that the predetermined security value may be a stored password, a value independent of the content of the flash memory.

The possibility that the hash or checksum may be independent of the content of the flash memory is simply not contemplated by Mirov or Cooper.

The fact that in both Mirov and Cooper the verification is dependent on the code content itself presents a potential vulnerability. If read errors are encountered when computing the checksum or hash as described by Cooper or Mirov, or if the component used to compute the checksum or hash is corrupted, there is an additional opportunity for the comparison to fail. The pending claimed subject matter avoids this possibility by omitting the checksum or hash computation. For this reason, the Applicant submits that the currently pending claims are patentable over the cited art.

The pending claims are directed to a security feature

The pending claims are further differentiated from the Mirov and Cooper, whether they are taken alone or in combination, by the function implicitly recited therein. Claim 1 recites a "boot method for use in a mobile device having… a key value stored in a ***security location***, having an internal read-only memory storing… a ***predetermined security value***". Each of the other independent claims similarly recites a "security location" and a "predetermined security value".

As described in the pending application, there is a concern that a processor in a mobile device may be breached through a serial port line when a reset process is initiated, because upon reset the BootROM causes a serial port to be polled. If there is serial port activity, indicating that new code is to be downloaded, the BootROM will jump to a routine for downloading the new code; this new code may have complete access to other components in the mobile device (Application as published, paragraphs 4 and 5). It is therefore desirable to provide a "security feature" to reduce the likelihood of such a breach. (Application as published, paragraph 6). The present application therefore provides a security feature that comprises selective polling of the serial port, based on the result of a comparison between a value stored on an ASIC and a value stored in FLASH memory (Application as published, paragraph 8). The former value is a predetermined security value; the latter value is stored in a security location in FLASH memory (Application as published, paragraphs 8 and 9).

The "key value stored in the security location" and the "predetermined security value" recited in the claims thus provide a security feature that reduces the likelihood of a security breach in the manner described above; the serial port, as recited in the claims, is polled only if the recited security feature determines that it should be polled. This security feature is explicitly set out in the claims, which recite the "key value stored in the security location" and the "predetermined security value".

Mirov and Cooper, by contrast, are not directed to such a purpose. The step of calculating the checksum in Cooper is not directed to reducing the likelihood of a security breach by reducing the need for a port to be polled; it is directed to determining whether the FLASH memory has become corrupted (Cooper, col. 9, lines 30-46). Mirov, of course, is not directed to the polling of ports at all, let alone the possibility of a security breach by that means. The Applicant therefore submits that the claims as currently presented are patentable, as they are directed to a ***security*** measure to reduce security breaches via a serial port, whereas the cited art is not.

Response to Comments on Motivation

In view of the Examiner's observations regarding Cooper (Detailed Action, paragraph 27), the Applicant wishes to clarify its previous submissions regarding motivation.

The Applicant did ***not*** acknowledge that Cooper provided motivation to combine Mirov with Cooper. Rather, the Applicant's submission dated December 27, 2006 stated that Cooper must not provide any motivation at all, given the motivation identified in the Non-Final Action. In other words, the Applicant's submission was that the stated motivation to combine Mirov and Cooper was moot:

- In the previous Non-Final Action, it was stated that "[o]ne of ordinary skill in the art would have been motivated [to modify Mirov with Cooper] in order to achieve the advantage of allowing a flash ROM to be updated to a known valid state even if the computer is unable to boot" (Non-Final Action, Detailed Action, paragraph 5, page 3). This statement is repeated in the present Detailed Action at page 5, lines 5-7.

- In the Remarks submitted with the Amendment after Non-Final on December 27, 2006, the Applicant responded by pointing out that Cooper, col. 3, lines 23-26 already claimed to update flash ROM to a known valid state, even if the computer system is unable to boot".

The Applicant was making no admission regarding a motivation to combine the cited references; rather, the Applicant sought to point out that the stated motivation that the Examiner identified could not exist: there was, according to the passages of Cooper cited by the Examiner, no reason to add the teachings of Mirov to Cooper. Cooper can apparently accomplish this without the enhancement of Mirov. In view of the repeated assertion in the present Detailed Action, the Applicant repeats and relies on this argument.

Although the Examiner has aptly pointed out that a prior art reference may be modified for a different purpose than one directed to finding the solution provided by a claimed invention, the Applicant notes that the Supreme Court has recently emphasized the need to ***identify*** that purpose, which must be apparent:

> Often, it will be necessary... to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determined whether there was an ***apparent*** reason to combine the known elements in the fashion claimed by the patent at issue. (*KSR International Co.* v. *Teleflex, Inc.*, 550 U.S. ____ (2007) at 14; emphasis added)

As stated in the emphasized text in the above passage, the reason to combine the known elements must be ***apparent***, and must be identified. The Applicant believes that it has adequately refuted the only motivation identified in the Detailed Action: "allowing a flash ROM to be updated to a known valid state even if the computer is unable to boot" is not an apparent motivation to modify Mirov with Cooper, or even a reasonable motivation at all.

Furthermore, the applicant respectfully submits that the combination of Mirov with Cooper to yield subject matter allegedly within the scope of the pending claims is only possible through the impermissible application of hindsight. A skilled worker, looking forward from the appropriate date prior to the invention date of this application, would not have been motivated to make the stated modification in order to arrive at the claimed subject matter.

The rejections of all pending claims were premised on the assumption that there was a motivation to modify Mirov with Cooper. Thus, for the foregoing reasons, the applicant respectfully submits that all claims, as amended, are non-obvious and patentable over Mirov in view of Cooper: not only do Mirov and Cooper fail to teach or suggest *all* of the elements of the pending claims, but there is no motivation to modify Mirov with Cooper.

For the purpose of clarity, the Applicant has not, and does not, admit that the currently pending claims of the present application are directed to allowing a flash ROM to be updated to a known valid state even if the computer is unable to boot.

Response to Examiner's identification of AAPA

The Examiner identified several components that were said to form part of the Applicant's Admitted Prior Art (AAPA):

> AAPA does explicitly disclose reading a key value from a security location in the FLASH memory; comparing the key value to a predetermined security value stored in the internal memory; and selectively polling the serial port for activity based on the result of the comparison; wherein the polling is performed if the key value does not match the predetermined security value; and wherein the downloading is in response to a detection of serial port activity. (Detailed Action, page 7, lines 16-20)

The Applicant respectfully submits that the identification of these acts as AAPA is in error, since the above is not identified as prior art in the application. It is suggested that the word "not" was inadvertently omitted from the first line of the above paragraph (i.e., "AAPA does *not*…").

No new subject matter has been added by this amendment. Favourable reconsideration and allowance of this application are respectfully requested.

Executed at Toronto, Ontario, Canada, on May 22, 2007.

RICHARD C. MADTER
RYAN J. HICKEY
CHRISTOPHER PATTENDEN

Jenna L. Wilson
Registration No. 54908
(416) 971-7202, Ext. 290
Customer Number: 38735

JLW: